AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

[72 FR 65420, Nov. 20, 2007]

PART 29—PROTECTED CRITICAL INFRASTRUCTURE INFORMATION

Sec.

AUTHORITY: Pub. L. 107–296, 116 Stat. 2135 (6 U.S.C. 1 *et seq.*); 5 U.S.C. 301.

SOURCE: 71 FR 52271, Sept. 1, 2006, unless otherwise noted.

§ 29.1 Purpose and scope.

(a) *Purpose of this Part.* This part implements sections 211 through 215 of the Homeland Security Act of 2002 (HSA) through the establishment of uniform procedures for the receipt, care, and storage of Critical Infrastructure Information (CII) voluntarily submitted to the Department of Homeland Security (DHS). Title II, Subtitle B, of the Homeland Security Act is referred to herein as the Critical Infrastructure Information Act of 2002 (CII Act). Consistent with the statutory mission of DHS to prevent terrorist attacks within the United States and reduce the vulnerability of the United States to terrorism, DHS will encourage the voluntary submission of CII by safeguarding and protecting that information from unauthorized disclosure and by ensuring that such information is, as necessary, securely shared with State and local government pursuant to section 214(a) through (g) of the CII Act. As required by the CII Act, these rules establish procedures regarding:

(1) The acknowledgement of receipt by DHS of voluntarily submitted CII;

(2) The receipt, validation, handling, storage, proper marking and use of information as PCII;

(3) The safeguarding and maintenance of the confidentiality of such information, appropriate sharing of such information with State and local governments pursuant to section 214(a) through (g) of the HSA.

(4) The issuance of advisories, notices and warnings related to the protection of critical infrastructure or protected systems in such a manner as to protect from unauthorized disclosure the source of critical infrastructure information that forms the basis of the warning, and any information that is proprietary or business sensitive, might be used to identify the submitting person or entity, or is otherwise not appropriately in the public domain.

(b) *Scope.* The regulations in this part apply to all persons and entities that are authorized to handle, use, or store PCII or that otherwise accept receipt of PCII.

§ 29.2 Definitions.

For purposes of this part:

(a) *Critical Infrastructure* has the meaning stated in section 2 of the Homeland Security Act of 2002 (referencing the term used in section 1016(e) of Public Law 107–56 (42 U.S.C. 5195c(e)).

(b) *Critical Infrastructure Information*, or *CII*, has the same meaning as established in section 212 of the CII Act of 2002 and means information not customarily in the public domain and related to the security of critical infrastructure or protected systems, including documents, records or other information concerning:

(1) Actual, potential, or threatened interference with, attack on, compromise of, or incapacitation of critical infrastructure or protected systems by either physical or computer-based attack or other similar conduct (including the misuse of or unauthorized access to all types of communications and data transmission systems) that violates Federal, State, local, or tribal law, harms interstate commerce of the United States, or threatens public health or safety;

(2) The ability of any critical infrastructure or protected system to resist such interference, compromise, or incapacitation, including any planned or